REMARKS

Reconsideration of the rejection of claims 1-50 under 35 USC §103(a) in view of U.S. Patent Nos. 6,442,600 (Anderson) and 6,487,586 (Ogilvie) is respectfully requested on the grounds that neither the Anderson patent nor the Ogilvie patent discloses or suggests use of a viewer applet that:

> *is arranged to* ***decrypt*** *said electronic mail message to permit viewing of said electronic mail message before the occurrence of the* **date, time, or event selected by said originator of the electronic mail message**, *and to* ***prevent decryption*** *and viewing of said encrypted electronic mail message by said recipient after the occurrence of the date, time, or event selected by said originator of the electronic mail message,*

as recited in claims 1 and 41, much less such features recited in various other independent and dependent claims as downloading of the applet from a central mail server that encrypts the message (see, *e.g.*, independent claim 34), and streaming of the message from the central mail server so as to make it even more difficult to bypass the decryption prevention (see, *e.g.*, claim 38).

Instead, the Anderson patent teaches encryption and decryption of messages by a web browser, together with message deletion after an expiration date, ***but fails to associate the encryption/decryption feature of the browser with the message expiration feature*** (which is the basis principle of the present invention). Furthermore, the Ogilvie clearly does not suggest modification of the message deletion feature of Anderson by having the decryption software implement processing controls set by the sender since the Ogilvie patent merely discloses a method and system in which e-mail that is not read is automatically deleted.

The deficiencies of the applied references may be summarized as follows:

a. Anderson teaches encryption and decryption of e-mail, and deletion of messages after an expiration date, but does not think to use decryption (*i.e.*

prevention of decryption) to ensure that they message cannot survive the expiration date; and

b. Ogilvie places no limitations are placed on viewing of the message by the recipient, and therefore could not have suggested modification of the system of Anderson to use encryption/decryption to implement such limitations.

Indeed, inclusion of viewing controls would be **contrary** to the purpose of the Ogilvie system, **which is to avoid annoying persons who do not wish to read an e-mail by eliminating the need to positively delete the e-mail if deletion is desired**. The sender presumably wants recipients to read the e-mail and places absolutely no restrictions on doing so, but merely makes it convenient to automatically delete the e-mail if viewing is not desired. **In contrast, the claimed invention forces deletion even if viewing is desired, which is exactly contrary to Ogilvie**.

A more detailed discussion of the two references and the proposed combination follows:

1. The Anderson Patent

According to the Examiner, "*Anderson discloses an electronic mail system...comprising: a first computer...; recipient computers systems; ...a view applet (i.e. the message receiver 155 with the URL, the web browser software, see column 4 lines 13-16),*" and furthermore that "*Anderson discloses the electronic message (i.e. e-mail) includes minimum or maximum expiration time periods (i.e. time is attached to the electronic mail message prior to transmission over network, see column 3 lines 62-67) will cause the electronic message and all designated incarnations thereof to expire. Anderson also discloses the electronic message (i.e. e-mail) is encrypted so that it may only be viewed using said view applet (i.e. URL web browser) upon installation of said view applet on the recipient computers (i.e. element 160, 170, 180, see figure 1 and column 5 lines 25-30)*" [pages 2-3 of the Official Action].

The Examiner is correct that the Anderson patent discloses a web browser, expiration periods, and decryption. However, the invention is not, as suggested by the Examiner, a web browser, electronic message expiration, and decryption. The fact the Anderson teaches these elements is irrelevant to the invention. The applicant has not suggested that it invented either a web browser, message encryption, or message expiration. What the applicant has invented is a way to **ensure** electronic message expiration by causing the applet that decrypts the message to stop decrypting the message after an expiration date established by a sender of the message.

It might be possible, with respect to the broader claims, to interpret an "applet" as a browser. However, **no browser is equipped to prevent decryption of a message based on a date entered by a sender of the message, as claimed.** Furthermore, a number of claims recite the feature in which the applet is downloaded from a central mail server and cooperates with the mail server to implement the expiration by decrypting the message based on key exchange *with the server* (no conventional browser is downloaded from a mail server and implements an expiration date in cooperation with the server in the manner claimed).

Therefore, the Anderson patent does not disclose or suggest ANY features of the claimed combination. The Anderson patent teaches that web browsers read e-mail, and that e-mail can be encrypted. These teachings are not suggestive of the claimed prevention of decryption after an expiration date, streaming of a message form a central mail server so that the message is never stored on the recipient's computer (making decryption even more difficult), or other features of the invention. The invention is a specific use of encryption for the purpose of preventing reading of a message after an expiration date. Anderson teaches elements of the combination, but does not in any way suggest the combination. This is no different than using Ben Franklin's teachings of electricity to render the telegraph and light bulb obvious on the grounds that these inventions utilize electricity, and that electricity is known.

To the contrary, the Anderson patent teaches a message expiration method that does not involve encryption. It teaches encryption of messages, but does not suggest using that encryption to prevent reading of a message after the expiration date. Instead, it teaches, essentially, **voluntary** message deletion at the expiration date. It does not teach or suggest the basic principle of the invention, which is to effectively cause a message to expire by preventing decryption of the message after the expiration date. As pointed out in the previous response, the Anderson patent merely gives the recipient the option of having a message automatically deleted on the expiration date or of saving the message. The recipient is not prevented from doing anything that he or she wants to do with the message, and encryption is not involved in expiration of the message or in preventing the recipient from circumventing expiration controls by simply copying or saving the message and viewing it after the expiration date.

The purpose of the system of Anderson is to save **recipients** the trouble of storing, managing, and protecting received messages, as explained in col. 1, lines 20-29 and in particular in col. 1, lines 65 *et seq.* of the Anderson patent.

> *Some embodiments of the present invention provide a method and system for distributing electronic messages in an efficient manner using centralized storage and management. In particular, the system receives electronic messages to be distributed to one or more recipients, centrally stores a single copy of the message as well as various information about sending the message, and sends to each recipient a short indicator message to notify the recipient that the electronic message is available. The system then tracks and manages requests from the recipients to access the message by permitting access when appropriate, performing activities such as decrypting/encrypting the message if necessary, recording information about the access and about recipient instructions related to the message, archiving the message if necessary, and deleting the message when it is no longer needed. The recipient can also provide various instructions about actions to be taken with the message corresponding to an indicator, such as to save or delete the message or to forward the message to another recipient. In one embodiment, after all recipients have reviewed the message and no recipient has currently indicated to save the message (or all have indicated to delete the message), the system then deletes the single copy of the message).*

Nowhere does this passage disclose or suggest that tracking and management of messages is in response to controls selected by the originator or sender of the message **and implemented by means of encryption and a viewer applet on the recipient's computer**.

To implement the system of Anderson, there is no need for decryption to prevent viewing of a message except via a "viewer applet" that limits message access by the recipient. The only encryption provided for is encryption at the request of the recipient to limit viewing by third parties rather than the recipient. There are no limits on viewing of the message by the recipient, and any limitations that are selected by the message originator or sender are implemented by a message tracking table rather than a viewer applet, as claimed, that decrypts the message at the recipient's computer.

2. The Ogilvie Patent

Like the present invention, the Ogilvie patent discloses systems and methods for enabling an originator to designate an expiration date for e-mail. However, the reason that Ogilvie includes the expiration date is so that the recipient does not have to bother with deletion of the e-mail. **The recipient is free to over-ride the expiration date and continue viewing the e-mail**. In contrast, the claimed invention seeks to provide absolute originator-control of the expiration date, so that it is impossible for the recipient to prevent expiration. This is accomplished by encrypting the message so that it can only be read by a viewer applet arranged to implement the originator-controls.

Ogilvie does not anywhere mention the type of encryption that enables originator or sender control of message, or message wrapper, viewing. Furthermore, Ogilvie does not need such encryption since Ogilvie's controls are for the convenience of the recipient, with the recipient preferably being given the option of over-riding the control. This makes sense since Ogilvie is designed to make spam more recipient friendly, *and it is to the sender's advantage in such cases if the recipient does desire to over-ride a control and keep the message in question.*

Col. 5, lines 52-54 of the Ogilvie patent explains how the message deletion is implemented by including a removal code in the recipient's browser or email reception program, so that the recipient does not need to actively delete the message if he/she does not wish to save it. **This is purely voluntary and clearly does not require or use encryption/decryption prevention for implementation.** Instead, as described in col. 6, lines 8-13 of the Ogilvie patent, the recipient has the **option** of deleting a message automatically after a predetermined period, such as 24 hours after receipt. **Nowhere do these passages suggest encryption of the message, much less control of information in the email *wrapper* as claimed**. Since Ogilvie is simply concerned with convenience, and not with *preventing* a recipient from keeping a message longer than the designated expiration date, there is ***no need*** for Ogilvie to encrypt messages, or the message wrapper, as claimed.

3. Combination of Anderson and Ogilvie

Neither the Anderson patent nor the Ogilvie patent discloses or suggests the claimed viewer applet that uses **encryption/decryption** to **positively prevent** viewing of a message **and all incarnations of the message** based on conditions established by the message originator.

Instead of relying on a viewer applet installed on the recipient's computer (and encryption of the message to ensure that it can only be read using the viewer applet, the Ogilvie teaches voluntary (*albeit* automatic) deletion of a message at the expiration of a period set by the *recipient* and not the message originator. In the systems taught by **both** the Anderson patent and the Ogilvie patent, expiration is **voluntary** on the part of the ***recipient***, and there is again no need to use encryption to prevent viewing of a message *by* the ***recipient***.

The claimed invention uses a viewer applet to enable reading of a message until the preset date sent by the user. **Each of the patents applied by the Examiner also causes message expiration, but neither does it in the claimed manner, by using encryption to prevent the recipient from a viewing a message in a manner contrary to the conditions set**

by the sender. While encryption of messages is of course, encryption is used to prevent third parties from a viewing a message. There is no suggestion in any of the references of record of using encryption to control how the intended recipient views a message.

Although the use of encryption to control how an intended recipient views a message is believed to be positively set forth in each of the original claims, claims 1 and 41 have nevertheless been amended to further emphasize this point. In particular, each of the claims now even more positively recites that the same applet that decrypts the message also prevents viewing by not decrypting of the message.

In addition, neither the Anderson nor Ogilvie patents suggests the use of a central server to **stream** messages to an expiration-date controlling viewer applet on the recipient's computer. As explained above, the Anderson patent discloses deletion of a saved message by a central "tracking table" associated with a "message distributor." Prevention of viewing is not carried out by a viewer applet on the recipient's computer. This is not only contrary to the claimed invention, but also fundamentally different than the approach taken by Ogilvie, in which the central server that forwards e-mail plays no part in the message expiration and/or control. **According to the streaming method, the message is never present on the recipient's computer, and therefore there is no need to "destroy" or delete the message, as in the systems of Anderson and Ogilvie**.

Because neither the Anderson patent nor the Ogilvie patent discloses or suggests control of message expiration by means of a viewer applet on the recipient's computer that provides access to the message prior to the expiration date through the use of decryption, and that prevents such access by ceasing decryption after the expiration date, withdrawal of the rejection under 35 USC §103(a) is respectfully requested.

Having thus overcome each of the rejections made in the Official Action, expedited passage of the application to issue is requested.

Should the Examiner nevertheless feel that issues remain that could possibly be resolved in a telephone or personal interview, the Examiner is invited to contact the undersigned at any time to arrange such an interview.

Respectfully submitted,

BACON & THOMAS, PLLC

Date: January 6, 2005

By: BENJAMIN E. URCIA
Registration No. 33,805

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314
Telephone: (703) 683-0500

NWB:S:\Producer\ben\Pending 1...PU\LEONARD390363\a04.wpd